Chapter 9
Restricted Data

Section 1. Introduction

9-100. General. This chapter of the NISPOMSUP addresses those supplemental security requirements for SECRET Restricted Data (SRD) and TOP SECRET Restricted Data (TSRD) information which have been identified as being sufficiently sensitive to necessitate security standards above and beyond those mandated by the NISPOM baseline document. ***Hereafter these are referred to as Critical SRD or TSRD. CONFIDENTIAL RD and all classification levels of Formerly Restricted Data shall be protected in accordance with the requirements in the NISPOM baseline document.*** In addition to those requirements in Chapter 9 of the NISPOM, this chapter prescribes the supplemental requirements for the protection of Critical SRD and TSRD information. Neither the NISPOM nor the NISPOMSUP are to be construed to apply to the safeguarding requirements for Special Nuclear Material, Nuclear Explosive Like Assemblies, or Nuclear Weapons.

9-101. Requirements. Under the authority of the Atomic Energy Act of 1954, the Secretary of Energy, using his/her authority over Restricted Data, may issue orders, guides, and manuals concerning protection of Restricted Data. These issuances serve as the basis for government-wide implementation procedures. However, these procedures of other agencies have not been endorsed by DOE. As a result of changes in the world situation, these policy issuances are currently under review by the Joint DOE/DOD Nuclear Weapons Information Access Authorization Review Group. Until the Review Group's recommendations are approved as policy by the Secretary of Energy, DOD contractors will continue to protect Critical SRD and TSRD in accordance with established contractual provisions. A revision of this chapter will be developed and promulgated following the results of the Joint DOE/DOD Nuclear Weapons Information Access Authorization Review Group. Nothing in this paragraph alters or abridges the authority of the Secretary of Energy under the Atomic Energy Act of 1954, as amended. DOD contracts awarded in the interim period dealing with the physics of nuclear weapons design, as specified in 9-101 .a through 9-101.i, will be reviewed by technically qualified representatives to determine if the contract involves the above specified Critical SRD or TSRD information. ***If so, this chapter's requirements will be included in the contractual document.*** DOE technical experts will be available to provide advice and assistance upon request by contracting agency representative. Should the results of the Joint DOE/DOD Nuclear Weapons Information Access Authorization Review Group modify the information specified in 9-101 .a through 9-101 .i, the affected contracts may be amended. ***For DOE contractors, Restricted Data will continue*** to ***be protected in accordance with the Department of Energy's 5600 series Safeguards and Security orders until the Review Group's recommendations are approved as policy by the Secretary of Energy and this chapter is revised to conform to the new policy.***

a. Theory of operation (hydrodynamic and nuclear) or completed design of thermonuclear weapons or their unique components. This definition includes specific information about the relative placement of components and their functions with regard to initiating and sustaining the thermonuclear reaction.

b. Theory of operation or complete design of fission weapons or their unique components. This definition includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiating system as they pertain to weapon design and theory.

c. Manufacturing and utilization information which reveals the theory of operation or design of the physics package.

d. Information concerning inertial confinement fusion which reveals or is indicative of weapon data.

e. Complete theory of operation, complete or partial design information revealing sensitive design features or information on energy conversion of a nuclear directed energy weapon. Sensitive information includes but is not limited to the nuclear energy converter, energy director, or other nuclear directed energy system or components outside the envelope of the nuclear source but within the envelope of the nuclear directed energy weapon.

f. Manufacturing and utilization information and output characteristics for **nuclear** energy converters, directors, or other nuclear directed energy weapon systems or components outside the envelope of the nuclear source and which do not comprehensively reveal the theory of operation, sensitive design features of the nuclear directed energy weapon or how the energy conversion takes place.

g. Nuclear weapon vulnerability assessment information concerning use control systems that reveals an exploitable design feature, or an exploitable system weakness or deficiency, **which** could be expected to permit the unauthorized use or detonation of a nuclear weapon.

h. Detailed design and functioning information of nuclear weapon use control systems and their components. Includes actual hardware and drawings that reveal design or theory of operation. This also includes use control information for passive and active systems as well as for disablement systems.

i. Access to specific categories of noise and quieting information, fuel manufacturing technology and broad policy or program direction associated with Naval Nuclear Propulsion Plants as approved by the Naval Nuclear Propulsion Program CSA.

9-102.

a. ***Contractors shall establish protective measures for the safeguarding of Critical SRD and TSRD in accordance with the requirements of this chapter. Where these requirements are not appropriate for protecting specific types or forms of material, compensatory provisions shall be developed and approved by the CSA, with the concurrence of DOE, as appropriate. Nothing in this NISPOMSUP shall be construed to contradict or inhibit compliance with the law or building codes.***

b. ***Access to Restricted Data shall be limited to persons who possess appropriate access authorization, or PCL, and who require such access (need-to-know) in the performance of official duties (i.e., have a verifiable need-to-know). For access to TOP SECRET Restricted Data, an individual must possess an active Q access authorization, or a final TOP SECRET PCL, based on a SSBI. For access to Critical SECRET Restricted Data, as defined in 9-101.a through 9-101.i, an individual must possess an active Q access authorization, or final TOP SECRET or SECRET PCL, based on a SSBI. Controls shall be established to detect and deter unauthorized access to Restricted Data.***

Section 2. Secure Working Areas

9-200. **Secure Working Areas.**

a. **General.** When not placed in approved storage, Critical SRI) and TSRD must be maintained in approved Secured Working Areas, and be constantly attended to by, or under the control of, a person or persons having the proper access authorization, or PCL, and a need-to-know, who are responsible for its protection.

b. **Requirements. Secure** Working Area boundaries shall be defined by physical barriers (e.g., fences, walls, doors). Protective personnel or other measures shall be used to control authorized access through designated entry portals and to deter unauthorized access to the area. A personnel identification system (e.g., security badge) shall be used as a control measure when there are more than 30 persons per shift. Entrance/Exit inspections for prohibited articles and/or Government property may be conducted by protective personnel. When access to a Secure Working Area is authorized for a person without appropriate access authorization or need-to-know, measures shall be taken to prevent compromise of classified matter. Access to safeguards and security interests within a Secure Working Area, when not in approved storage, is controlled by the custodian(s) or authorized **user(s).** Means shall be used to detect unauthorized intrusion appropriate to the classified matter under protection.

9-201. Barriers. ***Physical barriers shall be used to demarcate the boundaries of a Secure Working Area. Permanent barriers shall be used to enclose the area, except during construction or transient activities, when temporary barriers may be erected.*** Temporary barriers may be of any height and material that effectively impede access to the area.

a. **Walls.** ***Building materials shall offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction shall meet local building codes. Walls that constitute exterior barriers of Security Areas shall extend from the floor to the structural ceiling, unless equivalent means are used.***

(1) ***When transparent glazing material is used, visual access to the classified material shall be prevented by the use of drapes, blinds, or other means.***

(2) Insert-type panels (if used) shall be such that they cannot be removed from outside the area being protected without showing visual evidence of tampering.

b. **Ceilings and Floors.** ***Ceilings and floors shall be constructed of building materials that offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction shall meet local building codes.***

c. **Doors.** ***Doors and doorjambs shall provide the necessary barrier delay rating requi: by the applicable procedure. As a minimum, requirements shall include the following:***

(1) ***Doors with transparent glazing material may be used if visual access is not a security concern; however, they shall offer penetration resistance to, and evidence of, unauthorized entry into the area.***

(2) A sight baffle shall be used if visual access is a factor.

(3) An astragal shall be used where doors used in pairs meet.

(4) Door 10U vers, baffle plates, or astragals, when used, shall be reinforced and immovable from outside the area being protected.

d. **Windows.** ***The following requirements shall be applicable to windows:***

(1) When primary reliance is placed on windows as physical barriers, they shall offer penetration resistance to, and evidence of, unauthorized entry into the area.

(2) Frames shall be securely anchored in the walls, and windows shall be locked from the inside or installed in fixed (nonoperable) frames so the panes are not removable from outside the area being protected.

(3) ***Visual barriers shall be used if visual access is a factor.***

e. Unattended Openings.

(1) *Physical protection features shall be implemented at all locations where storm sewers, drainage swells, and site utilities intersect the fence perimeter.*

(2) *Unattended openings in security barriers, which meet the following criteria, must incorporate compensatory measures such as security bars: greater than 96 inches square* **(619.20** *square centimeters) in area and greater than 6 inches (15.24 centimeters) in the smallest dimension; and located within 18 feet (5.48 meters) of the ground, roof, or ledge of a lower Security Area; or located 14 feet (4.26 m) diagonally or directly opposite windows, fire escapes, roofs, or other openings in uncontrolled adjacent buildings; or located 6 feet (1.83 m) from uncontrolled openings in the same barrier.*

Section 3. Storage Requirements

9-300. General. *Custodians and authorized users of Critical SRD and TSRD are responsible for the protection and control of such matter.*

9-301. TSRD Storage. *TOP SECRET Restricted Data that is not under the personal control of an authorized person shall be stored within a security repository located within a Secure Working Area with CSA approved supplementary protection consistent with Chapter 5-307.a and 5-307.b of the NISPOM baseline. Authorized repositories are as follows:*

a. *In a locked, General Services Administration - approved security container.*

b. *In a vault or vault-type room.*

9-302. **Critical SRD Storage.** *Critical SRD shall be stored in a manner authorized for Top Secret Restricted Data matter or in one of the following ways:*

a. *In a locked General Services Administration-approved security container located within a Secure Working Area.*

b. *In a General Services Administration-approved security container, not located within a Secure Working Area, under supplemental protection (i.e., intrusion detection system protection or protective patrol).*

c. In a steel filing cabinet, not meeting General Services Administration requirements, but approved for use prior to the date of this NISPOMSUP, which may continue to be used until there is a need for replacement. It shall be equipped with a minimum of either an Underwriter Laboratories Group 1, built-in, changeable combination lock or a lock that meets Federal Specification FF-P-11O "Padlock, Changeable Combination. " Steel filing cabinets located within a Secure Working Area shall be under approved supplemental protection (i.e., intrusion detection system protection or protective patrol). If the steel filing cabinet is not located within a Secure Working Area, it shall be under intrusion detection system protection.